

BURSOR & FISHER, P.A.

Sarah N. Westcot (State Bar No. 264916)

701 Brickell Avenue, Suite 2100

Miami, FL 33131

Telephone: (305) 330-5512

Facsimile: (305) 676-9006

Email: swestcot@bursor.com

Counsel for Plaintiff

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

MARIA ROSE VOSS, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

SKINSPIRIT ESSENTIAL LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Maria Rose Voss (“Plaintiff”) brings this class action complaint on behalf of
 2 herself and all others similarly situated (the “Class Members”) against Defendant SkinSpirit
 3 Essential LLC (“SkinSpirit” or “Defendant”). Plaintiff brings this action based upon personal
 4 knowledge of the facts pertaining to herself, and on information and belief as to all other matters,
 5 by and through the investigation of undersigned counsel.

6 **NATURE OF THE ACTION**

7 1. This is a class action lawsuit brought on behalf of all California residents who
 8 accessed <https://www.skinspirit.com/> (the “Website”), to schedule a consultation for medical
 9 treatment and/or services.

10 2. Defendant is “the premier destination for medical aesthetics and skincare—for face
 11 and body . . . renowned for personalized service delivering safe, effective, medically-proven
 12 treatments”¹ Defendant provides an array of medical services and treatments to its patients,
 13 including various injectables, laser treatments, body contouring, and laser hair removal procedures.
 14 Defendant maintains an “expert staff of medical professionals” at each of its locations across more
 15 than a dozen states, including its 17 clinics in the state of California.²

16 3. When booking medical services online, patient privacy is crucial. Patients expect,
 17 as they should, that their information will be held in confidence and not shared with third parties
 18 without their knowledge or consent. The sensitive nature of information related to cosmetic
 19 medical procedures, such as those offered by Defendant, amplifies the need for privacy during
 20 online bookings. Medical procedures often involve deeply personal details about an individual’s
 21 physical appearance, struggles with body image, and health history. This information can be
 22 emotionally charged and stigmatizing, making the protection of such data especially critical.

23 4. Moreover, information concerning an individual’s healthcare, including medical
 24 procedures, is protected by state and federal law. Despite these protections, and unbeknownst to
 25 Plaintiff and Class Members, Defendant aided, employed, agreed, and conspired with LinkedIn to

26
 27 ¹ LINKEDIN, *SkinSpirit About*, <https://www.linkedin.com/company/skinspirit-skincare-clinic-&-spa/about/>.

28 ² SKINSPIRIT, *Our Story*, <https://www.skinspirit.com/skinspirit-company-story/>.

1 intercept sensitive and confidential communications sent and received by Plaintiff and Class
2 Members, including communications containing protected medical information. Plaintiff brings
3 this action for legal and equitable remedies resulting from these illegal actions.

4 **PARTIES**

5 5. Plaintiff is an adult citizen of the state of California, domiciled in San Francisco,
6 California.

7 6. Plaintiff has maintained a LinkedIn account at all relevant times when booking her
8 medical appointments on the Website.

9 7. Plaintiff has booked several appointments through the Website within the past two
10 years. For example, in or around December 1, 2023, Plaintiff navigated to Defendant's Website to
11 book an appointment for Botox treatment at Defendant's Presidio Heights location. During the
12 booking process, Plaintiff selected the state she wished to book the appointment in, the type of
13 procedure she was interested in, the specific procedure she wanted to have completed (Botox), the
14 reason for the procedure, the provider she wished to see, the day, and time for her appointment.
15 *See, e.g.,* Figures 1–5. Unbeknownst to Plaintiff, Defendant assisted LinkedIn with intercepting
16 Plaintiff's communications, including those that contained personally identifiable information
17 ("PII"), protected health information ("PHI"), and related confidential information. Defendant
18 assisted in these interceptions without Plaintiff's knowledge, consent, or express written
19 authorization. As a consequence of these interceptions, Plaintiff has received advertisements
20 marketing various cosmetic medical procedures, specifically targeted at Plaintiff as a result of
21 Defendant's disclosure of her medical booking information to LinkedIn. Defendant breached its
22 duties of confidentiality by unlawfully disclosing Plaintiff's PII and PHI.

23 8. Defendant SkinSpirit Essential LLC owns and operates a national network of
24 medical clinics specializing in a variety of cosmetic medical procedures. Defendant maintains
25 clinic locations in multiple states including 17 across the state of California. Defendant is a
26 Washington limited liability company with its principal place of business in Palo Alto, California.
27 Defendant owns and operates the Website, whereby consumers seeking to procure medical
28

1 procedures can schedule both virtual and in-person consultations for medical procedures, including
2 at clinics located within California.

3 **JURISDICTION AND VENUE**

4 9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §
5 1331 because it arises under a law of the United States (the Electronic Communications Privacy
6 Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law
7 claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges
8 that at least 100 people comprise the proposed class, that the combined claims of the proposed
9 class members exceed \$5,000,000 exclusive of interest and costs, and that at least one member of
10 the proposed class is a citizen of a state different from at least one defendant.

11 10. This Court has personal jurisdiction over the parties because the parties reside in
12 California. Further, Defendant has, at all times relevant hereto, systematically and continually
13 conducted business in California, including within this District, and intentionally availed itself of
14 the benefits and privileges of the California consumer market through the promotion, marketing,
15 and sale of its services to residents within this District and throughout California

16 11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant
17 conducts business in this District and its principal place of business is in this District.

18 **FACTUAL ALLEGATIONS**

19 **A. Background of the California Information Privacy Act**

20 12. The California Information Privacy Act ("CIPA"), California Penal Code § 630, *et*
21 *seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all
22 parties to a communication—read or learn the contents or meaning of any message, report, or
23 communication while the same is in transit or passing over any wire, line, or cable, or is being sent
24 from or received at any place within California.

25 13. To establish liability under California Penal Code § 631(a), a plaintiff need only
26 establish that the defendant, "by means of any machine, instrument, contrivance, or in any other
27 manner," does any of the following:
28

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

14. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new technologies" including computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

15. Under California Penal Code § 637.2, Plaintiff and Class Members may seek injunctive relief and statutory damages of \$5,000 per violation.

B. Background of the California Confidentiality of Medical Information Act

16. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), a "provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in

subdivision (b) or (c).” Cal. Civ. Code § 56.10(a). “An authorization for the release of medical information . . . shall be valid if it:

(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.

(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.

(c) Is signed and dated . . .

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.”

Cal. Civ. Code § 56.11.

17. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients’ personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).³ Similarly, if a negligent

³ “Every provider of health care . . . who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” Cal. Civ. Code § 56.101, subd. (a).

1 release occurs and medical information concerning a patient is improperly viewed or otherwise
2 accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

3 In addition to any other remedies available at law, any individual may bring an action
4 against any person or entity who has negligently released confidential information or
5 records concerning him or her in violation of this part, for either or both of the
6 following: [¶] (1) ... nominal damages of one thousand dollars (\$1,000). In order to
7 recover under this paragraph, it shall not be necessary that the plaintiff suffered or
8 was threatened with actual damages. [¶] (2) The amount of actual damages, if any,
9 sustained by the patient.

10 *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551, 174 Cal. Rptr. 3d 653, 656 (2014)
11 (quoting Cal. Civ. Code § 56.36(b)).

12 **C. LinkedIn's Platform and its Business Tools**

13 18. LinkedIn markets itself as “the world’s largest professional network on the
14 internet[.]”⁴ But LinkedIn is no longer simply a tool to help users find jobs or expand their
15 professional network. LinkedIn has moved into the marketing and advertising space and boasts of
16 its ability to allow potential advertisers to “[r]each 1 billion+ professionals around the world” via
17 its Marketing Solutions services.⁵ Recently, LinkedIn was projected as being responsible for
18 “roughly 0.9 percent of the global ad revenue” which included approximately \$5.91 billion in
19 advertising revenue in 2022.⁶

20 19. According to LinkedIn, “[t]argeting is a foundational element of running a
21 successful advertising campaign — [g]etting your targeting right leads to higher engagement, and
22 ultimately, higher conversion rates.”⁷ Targeting refers to ensuring that advertisements are targeted
23 to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn’s
24 Marketing Solutions services allow potential advertisers to “[b]uild strategic campaigns” targeting

25 ⁴ LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?,
26 <https://www.linkedin.com/help/linkedin/answer/a548441#>.

27 ⁵ LINKEDIN, MARKETING SOLUTIONS, <https://business.linkedin.com/marketing-solutions>.

28 ⁶ Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023),
<https://www.statista.com/statistics/275933/linkedins-advertising-revenue>.

⁷ LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3,
<https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf>.

specific users.⁸ LinkedIn’s “marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users].”⁹

20. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals’ demographics, intent, behavior, engagement, interests, buying decisions, and more.¹⁰

21. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn’s Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.¹¹

22. Such information is extremely valuable to marketers and advertisers because the inferences derived from users’ personal information and communications allows marketers and advertisers, including healthcare providers and insurance companies, to target potential customers.¹²

23. For example, through the use of LinkedIn’s Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to “reach

⁸ LINKEDIN, *supra* note 5.

⁹ LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, <https://www.linkedin.com/help/lms/answer/a421454>.

¹⁰ See LINKEDIN, MARKETING SOLUTIONS, <https://business.linkedin.com/marketing-solutions/audience> (“Target audiences through demographic marketing[,]” “Zero in on intent, behavior, engagement, interests, and more[,]” and “Reach the LinkedIn audience involved in the buying decision”).

¹¹ See *id.*

¹² LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy> (“We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads.”); LINKEDIN, ACCOUNT TARGETING, <https://business.linkedin.com/marketing-solutions/ad-targeting> (“Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests”); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf> (“BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers.”); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, <https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf> (listing “potential customers” as “Common audiences” for insurance sector).

millions of professionals across multiple touchpoints.”¹³ According to Broc Munro of Microsoft, “[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don’t spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising.”¹⁴

24. In July 2022, “LinkedIn Marketing Solutions surpassed \$5 billion in annual revenue[.]”¹⁵ That figure is “expected to further grow to reach 10.35 billion U.S. dollars by 2027.”¹⁶

25. According to LinkedIn, the LinkedIn Insight Tag is “[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences.”¹⁷ LinkedIn represents that the LinkedIn Insight Tag “enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors.”¹⁸

26. LinkedIn’s current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.¹⁹ A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.²⁰ LinkedIn “recommend[s] using the JavaScript-based Insight Tag or Conversions API” because third-party cookie settings are being

¹³ LINKEDIN, ACCOUNT TARGETING, <https://business.linkedin.com/marketing-solutions/ad-targeting>.

¹⁴ LINKEDIN, LINKEDIN AUDIENCE NETWORK, <https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network>.

¹⁵ *LinkedIn Business Highlights from Microsoft’s FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), <https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.>

¹⁶ Dencheva, *supra* note 6.

¹⁷ LINKEDIN, INSIGHT TAG, <https://business.linkedin.com/marketing-solutions/insight-tag>.

¹⁸ LINKEDIN, LINKEDIN INSIGHT TAG FAQs, <https://www.linkedin.com/help/lms/answer/a427660>.

¹⁹ LINKEDIN, *supra* note 17.

²⁰ *Id.* (“It’s important for advertisers to prepare for these changes by switching to JavaScript tags and enabling ‘enhanced conversion tracking’ in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.”).

1 deprecated across the industry.²¹ Embedding the JavaScript as a first-party cookie causes users’
2 browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited,
3 rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of
4 modern web browsers do not prevent LinkedIn from collecting data through its software.²² Instead,
5 the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party
6 cookies.

7 27. When a user who has signed in to LinkedIn (even if the user subsequently logs out)
8 is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent
9 using cookies, which includes information about the user’s actions on the website.

10 28. These cookies also include data that differentiate users from one another and can be
11 used to link the data collected to the user’s LinkedIn profile.

12 29. The HTTP request about an individual who has previously signed into LinkedIn
13 includes requests from the “li_sugr” and “lms_ads” cookies. Each of these cookies are used by
14 LinkedIn “to identify LinkedIn Members off LinkedIn” for advertising purposes.²³

15 30. For example, the “li_sugr” cookie is “[u]sed to make a probabilistic match of a
16 user’s identity.”²⁴ Similarly, the “lms_ads” cookie is “[u]sed to identify LinkedIn Members off
17 LinkedIn for advertising.”²⁵

18 31. A LinkedIn profile contains information including an individual’s first and last
19 name, place of work, contact information, and other personal details. Based on information it
20 obtains through the LinkedIn Insight Tag, which Defendant installed on the Website, LinkedIn is
21 able to target its account holders for advertising.

22 32. LinkedIn never receives consent from users to intercept and collect electronic
23 communications containing their sensitive and unlawfully disclosed information. In fact, LinkedIn
24

25 ²¹ *See id.*

26 ²² *See id.*

27 ²³ LINKEDIN, LINKEDIN COOKIE TABLE, <https://www.linkedin.com/legal/l/cookie-table>.

28 ²⁴ *See id.*

²⁵ *See id.*

1 expressly warrants the opposite. Similarly, Defendant never receives consent from users to share
2 information with LinkedIn.

3 33. When first signing up, a user agrees to the User Agreement.²⁶ By using or
4 continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy
5 Policy²⁷ and the Cookie Policy.²⁸

6 34. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect
7 the world's professionals Central to this mission is our commitment to be transparent about
8 the data we collect about you, how it is used and with whom it is shared."²⁹

9 35. The Privacy Policy goes on to describe what data LinkedIn collects from various
10 sources, including cookies and similar technologies.³⁰ LinkedIn states "we use cookies and similar
11 technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your
12 device(s) on, off and across different services and devices where you have engaged with our
13 Services. We also allow some others to use cookies as described in our Cookie Policy."³¹

14 36. However, LinkedIn offers an express representation: "**We will only collect and**
15 **process personal data about you where we have lawful bases.**"³²

16 37. Users never choose to provide sensitive information to LinkedIn because, among
17 other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if
18 so, what sensitive personal data it collects.

23 ²⁶ LINKEDIN, USER AGREEMENT, <https://www.linkedin.com/legal/user-agreement>.

24 ²⁷ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

25 ²⁸ LINKEDIN, COOKIE POLICY, <https://www.linkedin.com/legal/cookie-policy>.

26 ²⁹ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy>.

27 ³⁰ *Id.*

28 ³¹ *Id.*

³² *Id.* (emphasis added).

D. How Defendant Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted with Intercepting Communications

38. Defendant's patients access the Website to book consultations for various medical procedures. To begin, patients click a book now button on the Website, which allows them to pick which state they would like to book their consultation in. *See* Figures 1–2.

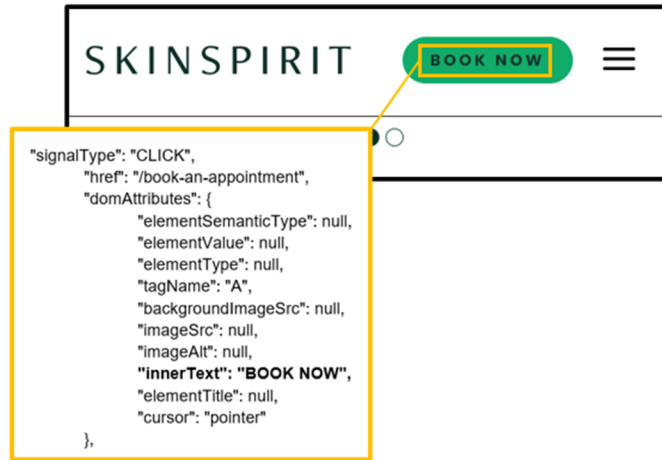


Figure 1: Screenshot of Defendant's Website with pixel interceptions overlaid (confirmable with developer tools)



Figure 2: Screenshot of Defendant's Website with pixel interceptions overlaid (confirmable with developer tools)

39. Unbeknownst to patients, LinkedIn was tracking their activity the moment they entered the Defendant's Website.

40. For example, Defendant embedded the LinkedIn Insight Tag on the Website, which allowed LinkedIn to intercept and record "click" events. Click events detail information about which page on the Website the patient was viewing as well as the selections they were making. LinkedIn intercepts information including the state the patient is booking the appointment in, the type of procedure they were interested in, the specific procedure they wanted to have completed, the reason for the procedure, the provider they wished to see, the day, and time for the patient's appointment. *See* Figures 1–5.

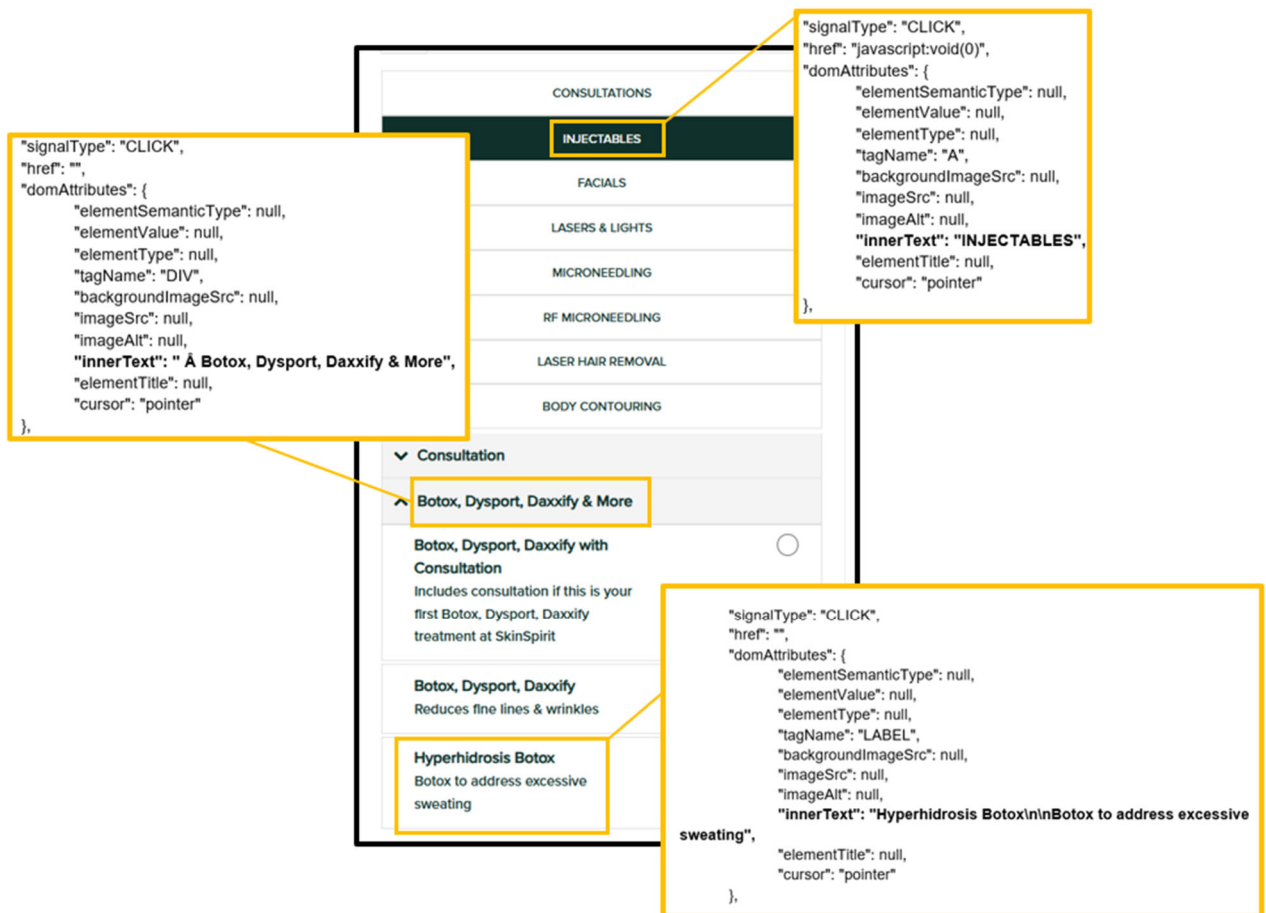


Figure 3: Screenshot of Defendant's Website with pixel interceptions overlaid (confirmable with developer tools)

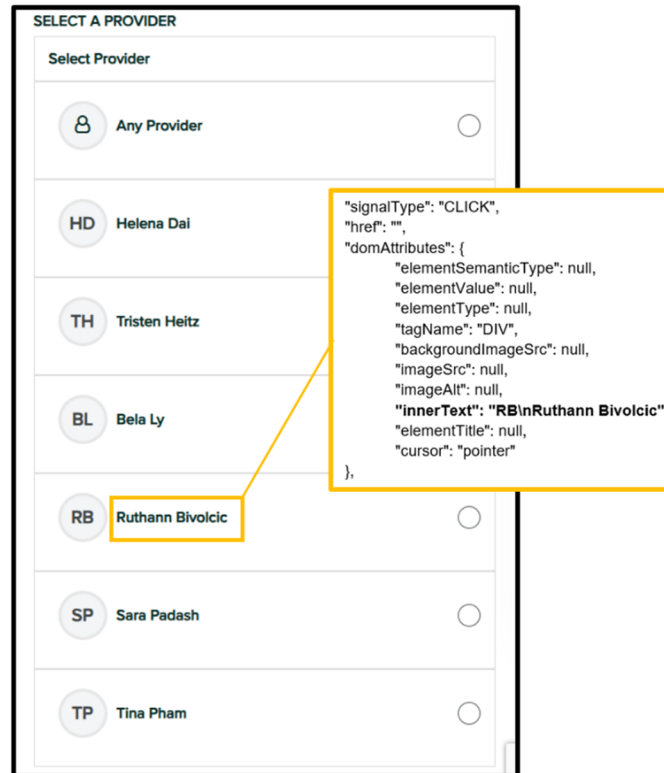


Figure 4: Screenshot of Defendant's Website with pixel interceptions overlaid (confirmable with developer tools)

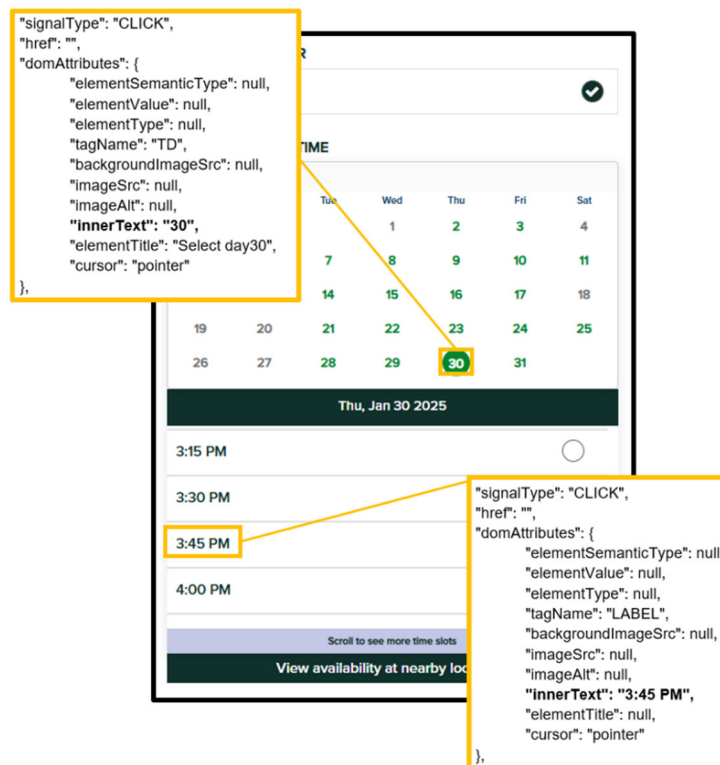


Figure 5: Screenshot of Defendant's Website with pixel interceptions overlaid (confirmable with developer tools)

1 41. By installing the LinkedIn Insight Tag on the Website, Defendant assisted LinkedIn
2 with intercepting patients' confidential information related to their medical appointments in order
3 to monetize that data for targeted advertising

4 42. As shown in Figures 2 through 5, LinkedIn intercepts several pieces of confidential
5 information, including the state the appointment is in, the type of procedure a patient is interested
6 in, the specific procedure they want completed, the reason for the procedure, the provider they wish
7 to see, the day, and time for the appointment.

8 43. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn
9 utilizes to identify its account holders for targeted advertising.

10 44. LinkedIn incorporated the information it intercepted from Defendant's Website into
11 its marketing tools to fuel its targeted advertising service.

12 45. Plaintiff never consented, agreed, authorized, or otherwise permitted LinkedIn to
13 intercept her confidential health information.

14 46. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to
15 share her confidential health information.

16 47. By law, Plaintiff is entitled to privacy in her protected health information and
17 confidential communications. LinkedIn deprived Plaintiff of her privacy rights when it
18 implemented a system that surreptitiously tracked and recorded Plaintiff's and other online
19 consumers' confidential communications, personally identifiable information, and protected health
20 information.

21 **E. Warning on Tracking Codes on Health Care Websites**

22 48. The federal government has issued guidance warning that tracking codes like the
23 LinkedIn Insight Tag may violate federal privacy law when installed on healthcare websites such
24 as Defendant's. The statement titled, USE OF ONLINE TRACKING TECHNOLOGIES BY
25 HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (the "Bulletin"), was issued by
26
27
28

1 the Department of Health and Human Services' Office for Civil Rights ("OCR") in December
2 2022.³³

3 49. Healthcare organizations regulated under the Health Insurance Portability and
4 Accountability Act (HIPAA) may use third-party tracking tools, such as the LinkedIn Insight Tag,
5 in a limited way, to perform analysis on data key to operations. They are not permitted, however, to
6 use these tools in a way that may expose patients' PHI to these vendors. The Bulletin explains:

7 Regulated entities [those to which HIPAA applies] are not permitted to use tracking
8 technologies in a manner that would result in impermissible disclosures of PHI to
9 tracking technology vendors or any other violations of the HIPAA Rules. ***For***
10 ***example, disclosures of PHI to tracking technology vendors for marketing***
purposes, without individuals' HIPAA-compliant authorizations, would constitute
impermissible disclosures.³⁴

11 50. The bulletin discusses the types of harm that disclosure may cause to the patient:

12 An impermissible disclosure of an individual's PHI not only violates the Privacy Rule
13 but also may result in a wide range of additional harms to the individual or others.
14 For example, an impermissible disclosure of PHI may result in identity theft, financial
15 loss, ***discrimination, stigma, mental anguish, or other serious negative***
consequences to the reputation, health, or physical safety of the individual or to
others identified in the individual's PHI. Such disclosures can reveal incredibly
16 sensitive information about an individual, ***including diagnoses, frequency of visits***
to a therapist or other health care professionals, and where an individual seeks
medical treatment. While it has always been true that regulated entities may not
17 impermissibly disclose PHI to tracking technology vendors, ***because of the***
proliferation of tracking technologies collecting sensitive information, now more
than ever, it is critical for regulated entities to ensure that they disclose PHI only as
expressly permitted or required by the HIPAA Privacy Rule.³⁵

18 51. Plaintiff and Class members face the risks about which the government expresses
19 concern. Defendant disclosed the fact that Plaintiff's and Class members' booked body contouring
20 medical procedures on Defendant's Website, which in turn also discloses the health conditions for
21 which they seek a health care provider; the frequency with which they take steps relating to body
22

23 ³³ HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND
24 BUSINESS ASSOCIATES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

25 ³⁴ *Id.* (Emphasis added).

26 ³⁵ *Id.* (Emphasis added).

1 image; and where they seek medical treatment. This information is, as described by the OCR in its
2 bulletin, “highly sensitive.”

3 52. The Bulletin goes on to make clear how broad the government’s view of protected
4 information is. It explains:

5 This information might include an individual’s medical record number, home or
6 email address, or dates of appointments, as well as an individual’s IP address or
7 geographic location, medical device IDs, *or any unique identifying code*.³⁶

8 53. Crucially, that paragraph in the government’s Bulletin continues:

9 *All such [individually identifiable health information (“IIHI”)] collected on a*
10 *regulated entity’s website or mobile app generally is PHI, even if the individual*
11 *does not have an existing relationship with the regulated entity and even if the IIHI,*
12 *such as IP address or geographic location, does not include specific treatment or*
13 *billing information like dates and types of health care services. This is because,*
14 *when a regulated entity collects the individual’s IIHI through its website or mobile*
15 *app, the information connects the individual to the regulated entity (i.e., it is*
16 *indicative that the individual has received or will receive health care services or*
17 *benefits from the covered entity), and thus relates to the individual’s past, present,*
18 *or future health or health care or payment for care.*³⁷

19 54. Then, in July 2022, the Federal Trade Commission (“FTC”) and the Department of
20 Health and Human Services (“HHS”) issued a joint press release warning regulated entities about
21 the privacy and security risks arising from the use of online tracking technologies:

22 The Federal Trade Commission and the U.S. Department of Health and Human
23 Services’ Office for Civil Rights (OCR) are cautioning hospitals and telehealth
24 providers [regulated entities] about the privacy and security risks related to the use of
25 online tracking technologies integrated into their websites or mobile apps that may
26 be impermissibly disclosing consumers’ sensitive personal health data to third
27 parties.

28 “When consumers visit a hospital’s [regulated entity’s] website or seek telehealth
services, they should not have to worry that their most private and sensitive health
information may be disclosed to advertisers and other unnamed, hidden third parties,”
said Samuel Levine, Director of the FTC’s Bureau of Consumer Protection. “The
FTC is again serving notice that companies need to exercise extreme caution when
using online tracking technologies and that we will continue doing everything in our

³⁶ *Id.* (Emphasis added).

³⁷ *Id.* (Emphasis added).

1 powers to protect consumers' health information from potential misuse and
2 exploitation."

3 "Although online tracking technologies can be used for beneficial purposes, patients
4 and others should not have to sacrifice the privacy of their health information when
5 using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR
6 Director. "OCR continues to be concerned about impermissible disclosures of health
7 information to third parties and will use all of its resources to address this issue."

8 The two agencies sent the joint letter to approximately 130 [regulated entities]
9 hospital systems and telehealth providers to alert them about the risks and concerns
10 about the use of technologies, such as the Meta/Facebook pixel and Google Analytics,
11 that can track a user's online activities. These tracking technologies gather
12 identifiable information about users, usually without their knowledge and in ways
13 that are hard for users to avoid, as users interact with a website or mobile app.

14 In their letter, both agencies reiterated the risks posed by the unauthorized disclosure
15 of an individual's personal health information to third parties. For example, the
16 disclosure of such information could reveal sensitive information including health
17 conditions, diagnoses, medications, medical treatments, frequency of visits to health
18 care professionals, and where an individual seeks medical treatment.

19 ... Through its recent enforcement actions against BetterHelp, GoodRx and Premom,
20 as well as recent guidance from the FTC's Office of Technology, the FTC has put
21 companies on notice that they must monitor the flow of health information to third
22 parties that use tracking technologies integrated into websites and apps. The
23 unauthorized disclosure of such information may violate the FTC Act and could
24 constitute a breach of security under the FTC's Health Breach Notification Rule ...

25 .³⁸

26 Therefore, Defendant's conduct is directly contrary to clear pronouncements by the FTC and HHS.

27 55. In light of, and in addition to, the federal government's own issued guidance above,
28 news sources also warn that tracking code, like the LinkedIn Insight Tag, poses risks of violating
federal privacy law and HIPAA:

Federal regulators are warning [regulated entities] hospital systems and telehealth
providers about the data privacy risks of using third-party tracking technologies.

These services, like [LinkedIn Insight Tag] or Google Analytics, could violate the
Health Insurance Portability and Accountability Act (HIPAA) or Federal Trade
Commission (FTC) data security rules, officials said.

³⁸ FEDERAL TRADE COMMISSION, FTC AND HHS WARN HOSPITAL SYSTEMS AND TELEHEALTH PROVIDERS ABOUT PRIVACY AND SECURITY RISKS FROM ONLINE TRACKING TECHNOLOGIES, July 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

1 The FTC and the U.S. Department of Health and Human Services' Office for Civil
 2 Rights (OCR) issued a rare joint release announcing that 130 [regulated entities]
 3 hospital systems and telehealth providers received a letter warning them about the
 4 data privacy and security risks related to the use of online tracking technologies
 5 integrated into their websites or mobile apps ... "The compliance buck still stops with
 6 you. Furthermore, your company is legally responsible even if you don't use the data
 7 obtained through tracking technologies for marketing purposes."³⁹

8 Fierce Healthcare also spoke up in an April 3, 2023 article:

9 Nearly all nonfederal acute care hospitals' [regulated entities'] websites track and
 10 transfer data to a third party, potentially fueling the unwanted disclosures of patients'
 11 sensitive health information and opening up that [regulated entity] hospital to legal
 12 liability, according to a recently published University of Pennsylvania analysis.
 13 [https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205]. The census of
 14 more than 3,700 hospital [regulated entity] homepages found at least one third-party
 15 data transfer among 98.6% of the websites as well as at least one third-party cookie
 16 on 94.3%, researchers wrote in Health Affairs.

17 The hospitals' [regulated entities'] homepages had a median of 16 third-party
 18 transfers, more of which were found among medium-sized (100 to 499 beds)
 19 hospitals, nonprofit hospitals, urban hospitals, health system-affiliated hospitals and
 20 those that weren't serving the largest portion of patients in poverty, they wrote ...
 21 Many of these complaints cite Facebook parent company Meta's Pixel tracker, which
 22 a June 2022 investigation from The Markup [https://themarkup.org/pixel-
 23 hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-
 24 hospital-websites] detected on about a third of large hospitals' websites. That report
 25 found evidence that, in some instances, the sensitive data transferred to third parties
 26 met the criteria for a HIPAA violation.⁴⁰

27 Health Affairs also published an article in April 2023, stating:

28 By including third-party tracking code on their websites, hospitals [regulated entities]
 are facilitating the profiling of their patients by third parties. These practices can lead
 to dignitary harms, which occur when third parties gain access to sensitive health
 information that a person would not wish to share. These practices may also lead to

³⁹ Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, <https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google>.

⁴⁰ Dave Muoio, *Almost every hospital's homepage is sending visitors' data to third parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023, <https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds>.

1 increased health-related advertising that targets patients, as well as to legal liability
2 for hospitals [regulated entities].⁴¹

3 56. This is further evidence that the data that Defendant chose to share is protected PHI
4 and PII. The sharing of that information was a violation of Class members' rights.

5 **CLASS ACTION ALLEGATIONS**

6 57. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23
7 individually and on behalf of a class defined as all natural persons in the United States who, during
8 the class period, had a LinkedIn account and booked an appointment on the Website (the "Class").

9 58. Plaintiff also brings this action on behalf of a subclass defined as all natural persons
10 in California who, during the class period, had a LinkedIn account and booked an appointment on
11 the Website (the "California Subclass") (together with the Class, the "Classes").

12 59. Subject to additional information obtained through further investigation and
13 discovery, the above-described Classes may be modified or narrowed as appropriate, including
14 through the use of multi-state subclasses.

15 60. The "Class Period" is the time beginning on the date established by the Court's
16 determination of any applicable statute of limitations, after consideration of any tolling,
17 concealment, and accrual issues, and ending on the date of entry of judgment.

18 61. Excluded from the Classes is Defendant; any affiliate, parent, or subsidiary of
19 Defendant; any entity in which Defendant has a controlling interest; any officer, director, or
20 employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this
21 action; any judge to whom this case is assigned, his/her spouse and immediate family members;
22 and members of the judge's staff.

23 62. Numerosity. Members of the Classes are so numerous that joinder of all members is
24 impracticable. The exact number of Class Members is unknown to Plaintiff at this time; however,
25 it is estimated that there are at least thousands of individuals in the Classes. The identity of such
26 membership is readily ascertainable from Defendant's records.

27 ⁴¹ Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites Poses Privacy*
28 *Risks For Patients And Legal Liability For Hospitals*, HEALTH AFFAIRS, Vol. 42, No. 24, April
2023, <https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205>.

63. Typicality. Plaintiff's claims are typical of the claims of the Classes because Plaintiff used the Website to schedule a medical appointment and had her personally identifiable information and protected health information disclosed to LinkedIn without her express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

64. Adequacy. Plaintiff is prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation, generally, and in the emerging field of digital privacy litigation, specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

65. Commonality. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

- a. Whether Defendant intentionally tapped the lines of internet communication between patients and their healthcare provider;
- b. Whether the Website surreptitiously recorded personally identifiable information, protected health information, and related communications and subsequently, or simultaneously, disclosed that information to LinkedIn;
- c. Whether LinkedIn is a third-party eavesdropper;
- d. Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;
- e. Whether Defendant's conduct, which allowed LinkedIn—an unauthorized person—to view Plaintiff's and Class Members' personally identifiable information and protected health information, resulted in a breach of confidentiality;

- 1 f. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using
2 the LinkedIn Insight Tag to record and communicate patients' confidential medical
3 communications;
- 4 g. Whether Plaintiff and Class Members are entitled to damages under the ECPA,
5 CIPA, the CMIA, or any other relevant statute; and
- 6 h. Whether Defendant's actions violated Plaintiff's and Class Members' privacy rights
7 as provided by the California Constitution.

8 66. Superiority. Class action treatment is the superior method for the fair and efficient
9 adjudication of this controversy. Such treatment permits a large number of similarly situated
10 persons to prosecute their common claims in a single forum simultaneously, efficiently, and
11 without the unnecessary duplication of evidence, effort, or expense that numerous individual
12 actions would engender. The benefits of proceeding through the class mechanism, including
13 providing injured persons or entities a method for obtaining redress on claims that could not
14 practicably be pursued individually, substantially outweigh any potential difficulties in the
15 management of this class action. Plaintiff knows of no special difficulty to be encountered in
16 litigating this action that would preclude its maintenance as a class action.

17 **CLAIMS FOR RELIEF**

18 **COUNT I**

19 **Violation of the Electronic Communications Privacy Act, 20 18 U.S.C. § 2511(1)**

21 67. Plaintiff repeats the allegations contained in the paragraphs above as if fully set
22 forth herein and brings this count individually and on behalf of the members of the Class.

23 68. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional
24 interception of the content of any electronic communication. 18 U.S.C. § 2511.

25 69. The ECPA protects both sending and the receipt of communications.

26 70. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or
27 electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter
28 119.

71. The transmission of Plaintiff's private and confidential information to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

72. The transmission of the private and confidential information between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

73. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

74. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

75. The ECPA defines "electronic, mechanical, or other device," as "any device...which can be used to intercept a[n]...electronic communication[.]" 18 U.S.C. § 2510(5).

76. The following instruments constitute "devices" within the meaning of the ECPA:

- a. The computer codes and programs LinkedIn used to track Plaintiff and Class Members communications while they were navigating the Website;
- b. Plaintiff's and Class Members' browsers;
- c. Plaintiff's and Class Members' mobile devices;
- d. Defendant and LinkedIn's web and ad servers;
- e. The plan Defendant and LinkedIn carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

77. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

1 78. By utilizing and embedding the LinkedIn Insight Tag on its Website, Defendant
2 intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the
3 electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

4 79. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic
5 communications through the LinkedIn Insight Tag, which tracked, stored and unlawfully disclosed
6 Plaintiff's and Class Members' private and confidential information to third parties, such as
7 LinkedIn.

8 80. Defendant intercepted or assisted in the interception of communications that
9 include, but are not necessarily limited to, communications to/from Plaintiff and Class Members
10 regarding private and confidential information, including their LinkedIn account and treatment
11 information. This confidential information was then monetized for targeted advertising purposes.

12 81. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class
13 Members' electronic communications to affiliates and other third parties, while knowing or having
14 reason to know that the information was obtained through the interception of an electronic
15 communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

16 82. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class
17 Members' electronic communications, while knowing or having reason to know that the
18 information was obtained through the interception of an electronic communication in violation of
19 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

20 83. Defendant intentionally intercepted or intentionally assisted in the interception of
21 the contents of Plaintiff's and Class Members' electronic communications for the purpose of
22 committing a criminal or tortious act in violation of the Constitution or laws of the United States or
23 of any state, namely, invasion of privacy, among others.

24 84. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that
25 intercepts or causes interception to escape liability if the communication is intercepted for the
26 purpose of committing any tortious or criminal act in violation of the Constitution or laws of the
27 United States or of any State. Here, as alleged above, Defendant violated a provision of the Health
28 Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This

1 provision imposes a criminal penalty for knowingly disclosing individually identifiable health
 2 information (“IIHI”) to a third party. HIPAA defines IIHI as:

3 any information, including demographic information collected from an individual,
 4 that—(A) is created or received by a health care provider ... (B) relates to the past,
 5 present, or future physical or mental health or condition of an individual, the
 6 provision of health care to an individual, or the past, present, or future payment for
 7 the provision of health care to an individual, and (i) identifies the individual; or (ii)
 8 with respect to which there is a reasonable basis to believe that the information can
 9 be used to identify the individual.⁴²

10 85. Plaintiff’s information that Defendant assisted LinkedIn in intercepting qualifies as
 11 IIHI, and Defendant violated Plaintiff’s and Class Members’ expectations of privacy. Such
 12 conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6.
 13 Defendant used the wire or electronic communications to increase their profit margins. Defendant
 14 specifically used the LinkedIn Insight Tag to track and utilize Plaintiff’s and Class Members’
 15 private and confidential information for financial gain.

16 86. Defendant was not acting under the color of law to intercept Plaintiff’s and Class
 17 Members’ wire or electronic communications.

18 87. Plaintiff and Class Members did not authorize Defendant to acquire the content of
 19 their communications for purposes of invading Plaintiff’s and Class Members’ privacy through the
 20 LinkedIn Insight Tag. Plaintiff and Class Members had a reasonable expectation that Defendant
 21 would not intercept or assist in the interception of their private and confidential information
 22 without their knowledge or consent.

23 88. The foregoing acts and omission therefore constitute numerous violations of 18
 24 U.S.C. § 2511(1), *et seq.*

25 89. As a result of each and every violation thereof, on behalf of herself and the Class,
 26 Plaintiff seeks statutory damages of \$10,000 or \$100 per day for each violation of 18 U.S.C. §
 27 2510, *et seq.* under 18 U.S.C. § 2520.

28 ⁴² 42 U.S.C. § 1320d-6.

COUNT II
**Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631**

90. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Subclass.

91. The California Invasion of Privacy Act (“CIPA”) is codified at California Penal Code sections 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to “protect the right of privacy of the people of [California]” from the threat posed by “advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications” Cal. Penal Code § 630.

92. A person violates California Penal Code § 631(a), if:

by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

93. Further, a person violates Section 631(a) if s/he “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned” in the preceding paragraph. *Id.*

94. To avoid liability under Section 631(a), a defendant must show it had the consent of **all** parties to a communication.

95. At all relevant times, Defendant aided, agreed with, and conspired with LinkedIn to track and intercept Plaintiff’s and Class Members’ internet communications while accessing the

1 Website. These communications were intercepted without the authorization and consent of Plaintiff
2 and Class Members.

3 96. Defendant, when aiding and assisting LinkedIn's wiretapping and eavesdropping,
4 intended to help LinkedIn learn some meaning of the content in the URLs and the content the
5 visitor requested.

6 97. The following items constitute "machine[s], instrument[s], or contrivance[s]" under
7 the CIPA, and even if they do not, the LinkedIn Insight Tag falls under the broad catch-all category
8 of "any other manner":

- 9 a. The computer codes and programs LinkedIn used to track Plaintiff and Class
10 Members' communications while they were navigating the Website
- 11 b. Plaintiff's and Class Members' browsers;
- 12 c. Plaintiff's and Class Members' computing and mobile devices;
- 13 d. LinkedIn's web and ad servers;
- 14 e. The web and ad-servers from which LinkedIn tracked and intercepted
15 Plaintiff's and Class Members' communications while they were using a web
16 browser to access or navigate the Website;
- 17 f. The computer codes and programs used by LinkedIn to effectuate its tracking
18 and interception of Plaintiff's and Class Members' communications while
19 they were using a browser to visit the Website; and
- 20 g. The plan LinkedIn carried out to effectuate its tracking and interception of
21 Plaintiff's and Class Members' communications while they were using a web
22 browser or mobile device to visit the Website.

23 98. The information that Defendant transmitted using the LinkedIn Insight Tag,
24 including the appointment location, the type of procedure a patient is interested in, the specific
25 procedure they want completed, the reason for the procedure, the provider they wish to see, the
26 day, and time for the appointment constituted sensitive and confidential personally identifiable
27 information.
28

99. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its customers' sensitive and confidential online communications through the Website without their consent.

100. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, \$5,000 dollars per violation or three times the amount of actual damages. Additionally, California Penal Code section 637.2 specifically states that “[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.”

101. Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT III
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56.10

102. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

103. Under the California Confidentiality of Medical Information Act, California Civil Code section 56.10 (“CMIA”), providers of health care are prohibited from disclosing medical information relating to their patients without a patient’s authorization. Medical information refers to:

any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient’s medical history, mental or physical condition, or treatment. “Individually Identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual . . .

104. Plaintiff and Class Members are patients under the definition of the CMIA because Plaintiff and Class Members received “health care services from a provider of health care” and the

1 information Defendant shared to LinkedIn was “medical information pertain[ing]” to Plaintiff and
2 Class Members. Cal. Civ. Code § 56.05(m).

3 105. Defendant is a “provider of health care” as defined in California Civil Code section
4 56.05(p) because Defendant offers various cosmetic medical services. Defendant is also considered
5 a “provider of health care” under California Civil Code section 56.06, subdivisions (a) and (b),
6 because Defendant’s Website maintains medical information and offers software to consumers that
7 is designed to maintain medical information for the purposes of allowing its users to manage their
8 information or make the information available to a health care provider, of for the diagnoses,
9 treatment, or management of a medical condition.

10 106. Therefore, as a provider of health care, Defendant is subject to the requirements of
11 the CMIA and had an ongoing obligation to comply with the CMIA’s requirements regarding the
12 maintenance of its user’s medical information.

13 107. As set forth hereinabove, the li_sugr and lms_ads cookies are identifiers sufficient
14 to allow identification of an individual. Along with patients’ li_sugr and lms_ads cookies,
15 Defendant disclosed to LinkedIn several pieces of information regarding its patients’ use of
16 Defendant’s Website, which, on information and belief, included, but was not limited to: patient
17 medical conditions and treatment patients were seeking such as scheduling medical consultations
18 searched for by customers.

19 108. This patient information was derived from a provider of health care regarding
20 patients’ medical treatment and physical condition. Accordingly, it constituted medical information
21 pursuant to the CMIA.

22 109. As demonstrated hereinabove, Defendant failed to obtain its patients’ valid
23 authorization for the disclosure of medical information.

24 110. Pursuant to CMIA section 56.11, a valid authorization for disclosure of medical
25 information must: (1) be “[c]learly separate from any other language present on the same page and
26 is executed by a signature which serves no other purpose than to execute the authorization;” (2) be
27 signed and dated by the patient or her representative; (3) state the name and function of the third
28 party that receives the information; and (4) state a specific date after which the authorization

1 expires. Accordingly, information set forth in Defendant's Website Privacy Policy does not qualify
2 as a valid authorization.

3 111. Based on the above, Defendant violated the CMIA by disclosing its patients'
4 medical information to LinkedIn.

5 112. Under the CMIA, a patient may recover compensatory damages, punitive damages
6 not to exceed \$3,000 dollars and attorneys' fees not to exceed \$1,000, and the costs of litigation for
7 any violating disclosure of medical information. Cal. Civ. Code §56.35. Alternatively, a patient
8 may recover nominal damages of \$1,000 for any negligent release of medical information. Cal.
9 Civ. Code §56.36.

10 113. Pursuant to California Penal Code section 637.2, Plaintiffs and Class Members have
11 been injured by the violations of California Penal Code section 635, and each seek damages for the
12 greater of \$5,000 or three times the amount of actual damages, as well as injunctive relief.

13 **COUNT IV**

14 **Invasion of Privacy Under California's Constitution**

15 114. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set
16 forth herein and brings this claim individually and on behalf of the proposed California Subclass.

17 115. Plaintiff and Class Members have an interest in: (1) precluding the dissemination
18 and/or misuse of their sensitive, confidential online communications and protected health
19 information; and (2) making personal decisions and/or conducting personal activities without
20 observation, intrusion or interference, including, but not limited to, the right to visit and interact
21 with various internet sites without being subjected to wiretaps without Plaintiff's and Class
22 Members' knowledge or consent.

23 116. At all relevant times, by using the LinkedIn Insight Tag to record and communicate
24 patients' sensitive and confidential online medical communications, Defendant intentionally
25 invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

26 117. Plaintiff and Class Members had a reasonable expectation that their sensitive and
27 confidential online communications, identities, health information, and other data would remain
28 confidential, and that Defendant would not install wiretaps on the Website.

118. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable health information.

119. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

120. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For a determination that this action is a proper class action;
- (b) For an order certifying the Classes, naming Plaintiff as representative of the Classes, and naming Plaintiff's attorneys as Class Counsel to represent the Classes;
- (c) For an order declaring that Defendant's conduct violates the statutes referenced herein;
- (d) For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;
- (e) An award of statutory damages to the extent available;
- (f) For punitive damages, as warranted, in an amount to be determined at trial;
- (g) For prejudgment interest on all amounts awarded;
- (h) For injunctive relief as pleaded or as the Court may deem proper; and
- (i) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and the proposed Classes, demands a trial by jury for all of the claims asserted in this Complaint so triable.

1 Dated: December 12, 2024

Respectfully submitted,

2 **BURSOR & FISHER, P.A.**

3 By: /s/ Sarah N. Westcot

4 Sarah N. Westcot (State Bar No. 264916)

5 701 Brickell Ave., Suite 2100

6 Miami, FL 33131-2800

7 Telephone: (305) 330-5512

8 Facsimile: (305) 676-9006

Email: swestcot@bursor.com

9 *Counsel for Plaintiff*